APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,365	07/03/2001	Teng Pin Poo	1601457-0007	4356

7590 11/03/2004

White & Case, LLP
Attn: Patent Department
1155 Avenue of the Americas
New York, NY 10036

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 11/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/898,365	POO ET AL.
	Examiner	Art Unit
	Shewaye Gelagay	2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
 Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *July 3, 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>6,7/3/01;7,10/7/03</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

Claim Rejections - 35 USC § 101

1.   The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2.   Claims 1-22 are provisionally rejected under the judicially created doctrine of double patenting over claims 1, 5, 11 and 17 of copending Application No. 09/898,310.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '310 teaches all the claims limitation except the differences that are underlined in the following table:

Application 09/898365	Application 09/898310
1. A portable device comprising: a microprocessor; a non-volatile memory coupled to the microprocessor; and a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.	1. A portable device comprising: a microprocessor; and a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to a restricted resource, the restricted resource having a communication port communicatively coupled to the portable device, is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise.

	5. The portable device as recited in claim 1 further comprising a non-volatile memory capable or storing biometrics information usable for authentication.
7. A portable device comprising: a bus; a microprocessor coupled to the bus; a non-volatile memory coupled to the bus; and a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker. 14. The portable device as recited in claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module. 15. The portable device as recited in claim 7 wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.	11. A biometrics-based access control system for controlling access to a restricted resource, comprising: a portable device which includes a non-volatile memory and a biometrics-based authentication module coupled thereto, wherein the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise.
17. A biometrics-based authentication method implemented using a portable device, the method comprising the steps of: (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device; (b) retrieving a registered biometrics marker from a memory of the portable device, the	17. A biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, the method comprising the steps of: (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device; (b) retrieving a registered biometrics marker

registered biometrics marker having been stored therein during a registration process; (c) comparing the first biometrics marker against the registered biometrics marker; and (d) signaling an authentication success provided that a match is identified in said step (c). 20. The biometrics-based authentication method as recited in claim 17 wherein said step (d) comprises <u>granting the user access to the non-volatile memory.</u>	from a memory of the portable device, the registered biometrics marker having been stored therein during a registration process; (c) comparing the first biometrics marker against the registered biometrics marker; and (d) granting the user <u>access to the restricted resource</u> provided that a match is identified in said step (c).

a. Both '365 (claim 1) and '310 (claims 1 and 5) teach a portable device with a microprocessor and non-volatile memory with a biometric-based authentication module. The only exception is ***access to non-volatile memory*** as recited in '365 claim 1 and ***access to a restricted resource, the restricted resource having a communication port communicatively coupled to a portable device*** as recited in '310 claim 1.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by '310 **access to a restricted resource** to **access to a non-volatile memory** as disclosed in '365. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so because a non-volatile memory could also be a restricted resource in which access is granted or denied by using biometric authentication.

b. Both '365 (claims 7, 14 and 15) and '310 (claim 11) teach a portable device with a biometric-based authentication module wherein it is configured to capture a first biometrics marker, store the first biometrics marker, capture a second biometrics marker

and determine whether the second biometrics marker can be authenticated against the first biometrics marker. The only exceptions are *a bus* as recited in '365 (claim 7) *and access to non-volatile memory* as recited in '365 (claims 14 and 15) and *access to the restricted resource* as recited in '310 (claim 11).

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by '310 **access to a restricted resource** to **access to a non-volatile memory** as disclosed in '365. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so because a non-volatile memory could also be a restricted resource in which access is granted or denied by using biometric authentication.

In addition, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by '310 to include a bus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to transfer data among the components of a device system such as a microprocessor and a non-volatile memory.

c. Both '365 (claims 17 and 20) and '310 (claim 17) teach a biometric-based access control method comprising the steps of: obtaining first biometrics marker, retrieving a registered biometrics marker, comparing the first biometrics marker against the registered biometrics marker and granting the user access provided that a match is identified. The only exception is *access to non-volatile memory* as recited in '365 claim 20 and *access to a restricted resource* as recited in '310 claim 17.

However, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the device disclosed by '310 **access to a**

restricted resource to **access to a non-volatile memory** as disclosed in '365. This

modification would have been obvious because a person having ordinary skill in the art

would have been motivated to do so because a non-volatile memory could also be a

restricted resource in which access is granted or denied by using biometric

authentication.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1, 2, 4, 5, 7, 8,10, 11, 13-15, 17, 18, 20 and 21 are rejected under 35

U.S.C. 102(e) as being anticipated by Bialick et al. United States Letters Patent No.

6,088,802.

As per claim 1:

Bialick et al. teach a portable device comprising:

a microprocessor; and (Figure 8, item 801)

a biometrics-based authentication module coupled to and controlled by the

microprocessor (Col. 5; lines 1-2; the peripheral device also provides the capability to

accept biometric input to enable user authentication to the host computing device),

wherein access to a restricted resource, the restricted resource having a communication

port communicatively coupled to the portable device (see figure 6), is granted to a user

provided that the biometrics-based authentication module authenticates the user's

identity and wherein access to the restricted resource is denied to the user otherwise.

(Col. 14; lines 50-52; biometric user authentication to a host computing device is made

before allowing access to particular data stored on the host computing device.)

As per claim 2:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the

biometrics-based authentication module is a fingerprint authentication module. (Col. 14,

lines 26-28; a sensor for sensing the fingerprint of the finger, the content of the sensed

fingerprint being converted into digital data by the device.)

As per claim 4:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the

biometrics-based authentication module comprises a biometrics sensor fitted on one

surface of the portable device. (Col. 14, lines 48-49; a peripheral device includes a

biometric device which includes a sensor for sensing the fingerprint)

As per claim 5:

The rejection of claim 1 is incorporated and further Bialick et al. disclose a non-

volatile memory capable or storing biometrics information usable for authentication.

(Figure 8, item 803; Col. 16; lines 10-11; the first memory device can be a non-volatile

data storage device which can be used to store computer programs and persistent

data.)

As per claim 7:

Bialick et al. disclose a portable device comprising:

a bus; (Figure 6, item 609)

a microprocessor coupled to the bus; (Figure 8, item 801)

a non-volatile memory coupled to the bus (Col. 16; lines 10-11; the first memory

device can be a non-volatile data storage device which can be used to store computer

programs and persistent data.); and

a biometrics-based authentication module coupled to the bus, wherein under the

control of the microprocessor the biometrics-based authentication module is configured

to (1) capture a first biometrics marker; (Col. 14, lines 55-56; an appropriate library of

biometric data representing a predetermined group of people; which indicates obtaining

the biometrics of authorized users the first time) (2) store the first biometrics marker in

the non-volatile memory; (Col. 14; lines 57-58; the library data can be stored in a

memory device of the peripheral device) (3) capture a second biometrics marker;

(Col.14; line 54; obtain biometric data from a user) and (4) determine whether the

second biometrics marker can be authenticated against the first biometrics marker. (Col.

14; lines 50-52; biometric user authentication to a host computing device is made before

allowing access to particular data stored on the host computing device.)

As per claim 8:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28; a sensor for sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device.)

As per claim 10:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device. (Col. 14, lines 48-49; a peripheral device includes a biometric device which includes a sensor for sensing the fingerprint)

As per claim 11:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the non-volatile memory comprises flash memory. (Figure 8, item 803)

As per claim 13:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory. (Col. 14, lines 55-56; an appropriate library of biometric data representing a predetermined group of people; which indicates obtaining the biometrics of authorized users the first time)

As per claim 14:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a

portable device, wherein the microprocessor is configured to enable access to the non-

volatile memory upon a determination of authentication success by the biometrics-

based authentication module. (Col. 14; lines 50-52; biometric user authentication to a

host computing device is made before allowing access to particular data stored on the

host computing device.)

As per claim 15:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a

portable device, wherein the microprocessor is configured to disable access to the non-

volatile memory upon a determination of authentication failure by the biometrics-based

authentication module. . (Col. 14; lines 50-52; biometric user authentication to a host

computing device is made before allowing access to particular data stored on the host

computing device.)

As per claim 17:

Bialick et al. teach a biometrics-based authentication method implemented using

a portable device, the method comprising the steps of: (a) obtaining a first biometrics

marker from a user with a biometrics sensor installed on the portable device; (Col.14;

line 54; obtain biometric data from a user) (b) retrieving a registered biometrics marker

from a memory of the portable device, the registered biometrics marker having been

stored therein during a registration process; (Col. 14; lines 57-58; the library data can be

stored in a memory device of the peripheral device; the stored biometrics has to be

retrieved in order to compare it with the newly obtained biometrics) (c) comparing the

first biometrics marker against the registered biometrics marker; (Col. 14; lines 54-56;

comparing the biometric data to an appropriate library of biometric data representing a

predetermined group of people.) and (d) signaling an authentication success provided

that a match is identified in said step (c). (Col. 14; lines 50-52; biometric user

authentication to a host computing device is made before allowing access to particular

data stored on the host computing device.)

As per claim 18:

The rejection of claim 17 is incorporated and further Bialick et al. disclose

biometrics-based access control method, wherein the registered biometrics marker is a

fingerprint. (Col. 14, lines 26-28; a sensor for sensing the fingerprint of the finger, the

content of the sensed fingerprint being converted into digital data by the device.)

As per claim 20:

The rejection of claim 17 is incorporated and further Bialick et al. disclose the

step of denying the user access to the restricted resource provided that a match is not

identified in said step (c). (Col. 14; lines 50-52; biometric user authentication to a host

computing device is made before allowing access to particular data stored on the host

computing device. the user authentication is made in order to grant or deny access to

the host computer depending the result of the comparison)

As per claim 21:

The rejection of claim 17 is incorporated and further Bialick et al. disclose the

step of denying the user access to the non-volatile memory provided that a match is not

identified in said step (c). (Col. 14; lines 50-52; biometric user authentication to a host

computing device is made before allowing access to particular data stored on the host

computing device. the user authentication is made in order to grant or deny access to

the host computer depending the result of the comparison)

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed
> or described as set forth in section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are such that the subject
> matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was
> made.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

6.   Claims 6, 12, 16, 19 and 22 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Bialick et al. United States Letters Patent No. 6,088,802.

As per claim 6:

Bialick et al. teach all the subject matter as described above. Bialick et al. further

disclose the peripheral device driver can be implemented so that the user must

successfully enter an acceptable access code (e.g., a password or PIN) before the user

is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by

Bialick et al. is that, the microprocessor is configured to provide a bypass mechanism

for authentication upon a determination of authentication failure by the biometrics-based

authentication module. However, it would have been obvious to a person having

ordinary skill in the art at the time the invention was made to modify Bialick et al.'s

method to include a microprocessor that is configured to provide a bypass mechanism

for authentication upon a determination of authentication failure by the biometrics-based

authentication module. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated to do so by the suggestion

provided by Bialick et al., in order to use the security functionality, thus enabling a layer

of security that protects the integrity of the restricted resources.

As per claim 12:

Bialick et al. teach all the subject matter as described above. Bialick et al. further

disclose the peripheral device further configured to encrypt the first biometrics marker

before storing the first biometrics marker in the non-volatile memory.

However, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Bialick et al.'s method to include further

configured to encrypt the first biometrics marker before storing the first biometrics

marker in the non-volatile memory. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so by

the suggestion provided by Bialick et al., in order to enhance the security of the

biometrics-based access control method.

As per claim 16:

Bialick et al. teach all the subject matter as described above. Bialick et al. further

disclose the peripheral device driver can be implemented so that the user must

successfully enter an acceptable access code (e.g., a password or PIN) before the user

is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by

Bialick et al. is that, a bypass mechanism for authentication is provided upon a

determination of authentication failure by the biometrics-based authentication module.

However, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Bialick et al.'s method to include a bypass

mechanism for authentication is provided upon a determination of authentication failure

by the biometrics-based authentication module. This modification would have been

obvious because a person having ordinary skill in the art would have been motivated to

do so by the suggestion provided by Bialick et al., in order to use the security

functionality, thus enabling a layer of security that protects the integrity of the restricted

resources.

As per claim 19:

Bialick et al. teach all the subject matter as described above. Bialick et al. further

disclose the peripheral device can be used to encrypt or decrypt data stored. Not

explicitly disclosed by Bialick et al. is that, the registered biometrics marker is stored in an encrypted format.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include the registered biometrics marker is stored in an encrypted format. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to enhance the security of the biometrics-based access control method.

As per claim 22:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include providing the user with a bypass authentication procedure provided that a match is not identified in said step (c). This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

7.   Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Bialick et al. United States Letters Patent No. 6,088,802 and in view of Bjorn United

States Letters Patent No. 6,799,275 .

As per claim 3:

        Bialick et al. teach all the subject matter as described above. In addition, Bialick

et al. disclose a communication interfaces, such as a smart card interface, a serial

interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al.

is that the portable device, further comprising a universal serial bus (USB) connector for

coupling with another USB-compliant device.

        Bjorn in analogous art, however, teaches a device further comprising a universal

serial bus (USB) connector for coupling with another USB-compliant device. (Col. 2,

lines 59-60; the digital connection is a data bus, which conforms to a universal serial

bus (USB) standard.)

        Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the method disclosed by Bialick et al. to

include a device further comprising a universal serial bus (USB) connector for coupling

with another USB-compliant device. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so,

as suggested by Bjorn, in order to provide a faster transfer of digitized image.

As per claim 9:

        Bialick et al. teach all the subject matter as described above. In addition, Bialick

et al. disclose a communication interfaces, such as a smart card interface, a serial

interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. the portable device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector.

Bjorn in analogous art, however, teaches a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Bjorn, in order to provide a faster transfer of digitized image.

8.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a. Novoa et al. U.S. 6,636,973

    This reference pertains to improved security during log on process.

    b. Brown et al. U.S. 6,618,806

This reference pertains to a rule based biometric user authentication method and system in a computer network environment.

c. Baird, III et al. U.S. 6,732,278

This reference pertains to a device for providing access to a remote site through an authentication process during which a user password and biometrics are provided.

d. McKeeth U.S. 6,766,456

This reference pertains to a method and system for authenticating a user to access a computer system.

e. Burger U.S. 6,219,439

This reference pertains to a biometric authentication system which includes a dual input reader.

9.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 703-305-1338. The examiner can normally be reached on 8:00 am to 5:30 pm.
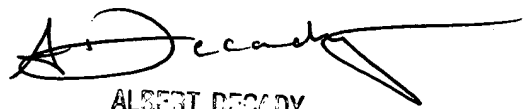
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay _SG_
Examiner
Art Unit 2133

10/18/04

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100